# 网络与信息安全技术A卷

一、 单项选择题（每小题2分，共20分）

## 1．信息安全的基本属性是＿＿＿。

## A. 保密性 B.完整性

C. 可用性、可控性、可靠性 D. A，B，C都是

## 2．假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于＿＿＿。

## A. 对称加密技术 B. 分组密码技术

## C. 公钥加密技术 D. 单向函数密码技术

## 3．密码学的目的是＿＿＿。

## A. 研究数据加密 B. 研究数据解密

## C. 研究数据保密 D. 研究信息安全

4．A方有一对密钥（KA公开，KA秘密），B方有一对密钥（KB公开，KB秘密），A方向B方发送数字签名M，对信息M加密为：M’= KB公开（KA秘密（M））。B方收到密文的解密方案是＿＿＿。

A. KB公开（KA秘密（M’）） B. KA公开（KA公开（M’））

C. KA公开（KB秘密（M’）） D. KB秘密（KA秘密（M’））

## 5．数字签名要预先使用单向Hash函数进行处理的原因是＿＿＿。

## A. 多一道加密工序使密文更难破译

## B. 提高密文的计算速度

## C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

## D. 保证密文能正确还原成明文

## 6．身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是＿＿。

## A. 身份鉴别是授权控制的基础

## B. 身份鉴别一般不用提供双向的认证

## C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

## D. 数字签名机制是实现身份鉴别的重要机制

7．防火墙用于将Internet和内部网络隔离＿＿＿。

A. 是防止Internet火灾的硬件设施

B. 是网络安全和信息安全的软件和硬件设施

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

## 8．PKI支持的服务不包括＿＿＿。

## A. 非对称密钥技术及证书管理 B. 目录服务

## C. 对称密钥的产生和分发 D. 访问控制服务

9．设哈希函数H有128个可能的输出(即输出长度为128位)，如果H的k个随机输入中至少有两个产生相同输出的概率大于0.5，则k约等于＿＿。

A．2128 B．264

C．232 D．2256

10．Bell-LaPadula模型的出发点是维护系统的＿＿＿，而Biba模型与Bell-LaPadula模型完全对立，它修正了Bell-LaPadula模型所忽略的信息的＿＿＿问题。它们存在共同的缺点：直接绑定主体与客体，授权工作困难。

A．保密性 可用性 B．可用性 保密性

C．保密性 完整性 D．完整性 保密性

二、 填空题（每空2分，共40分）

1．ISO 7498-2确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认。同时，ISO 7498-2也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换、业务填充机制、路由控制机制和公证机制。

2．古典密码包括 代替密码和置换密码两种，对称密码体制和非对称密码体制都属于现代密码体制。传统的密码系统主要存在两个缺点：一是 密钥管理与分配问题 ；二是 认证问题 。在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。

3．根据使用密码体制的不同可将数字签名分为 基于对称密码体制的数字签名 和 基于公钥密码体制的数字签名 ，根据其实现目的的不同，一般又可将其分为 直接数字签名 和 可仲裁数字签名 。

4. DES算法密钥是64位，其中密钥有效位是56位。RSA算法的安全是基于分解两个大素数的积的困难。

5．密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式有两种：一种是由中心集中生成，另一种是由个人分散生成。

6．认证技术包括站点认证、报文认证和身份认证，而身份认证的方法主要有口令、磁卡和智能卡、生理特征识别、零知识证明。

7．NAT的实现方式有三种，分别是静态转换、动态转换、端口多路复用。

8．数字签名是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

三、 简答题（每小题8分，共24分）

1、网络信息安全的含义？

答：网络信息安全是指利用[网络管理](http://baike.baidu.com/view/325702.htm" \t "_blank)控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可使用性受到保护。计算机网络安全包括两个方面，即[物理安全](http://baike.baidu.com/view/3153048.htm" \t "_blank)和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安安全包括信息的完整性、保密性和可用性。

2、什么是入侵检测系统？

答：[入侵检测](http://baike.baidu.com/view/16487.htm" \t "_blank)系统（简称“IDS”）是一种对[网络传输](http://baike.baidu.com/view/1542295.htm" \t "_blank)进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的[网络安全](http://baike.baidu.com/view/17495.htm" \t "_blank)设备。它与其他网络安全设备的不同之处便在于，IDS是一种积极主动的安全防护技术。 IDS最早出现在1980年4月。 1980年代中期，IDS逐渐发展成为入侵检测专家系统（IDES）。

3、请说明DES算法的基本过程？

答：DES加密算法特点：分组比较短、密钥太短、密码生命周期短、运算速度较慢。

DES工作的基本原理是，其入口参数有三个:key、data、mode。 key为加密解密使用的密钥，data为加密解密的数据，mode为其工作模式。当模式为加密模式时，明文按照64位进行分组，形成明文组，key用于对数据加密，当模式为解密模式时，key用于对数据解密。实际运用中，密钥只用到了64位中的56位，这样才具有高的安全性。

四、 分析题（16分）

1．下图表示的是P2DR2动态安全模型，请从信息安全安全角度分析此模型？

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

## 8．PKI支持的服务不包括＿＿＿。

## A. 非对称密钥技术及证书管理 B. 目录服务

## C. 对称密钥的产生和分发 D. 访问控制服务

9．设哈希函数H有128个可能的输出(即输出长度为128位)，如果H的k个随机输入中至少有两个产生相同输出的概率大于0.5，则k约等于＿＿。

A．2128 B．264

C．232 D．2256

10．Bell-LaPadula模型的出发点是维护系统的＿＿＿，而Biba模型与Bell-LaPadula模型完全对立，它修正了Bell-LaPadula模型所忽略的信息的＿＿＿问题。它们存在共同的缺点：直接绑定主体与客体，授权工作困难。

A．保密性 可用性 B．可用性 保密性

C．保密性 完整性 D．完整性 保密性

二、 填空题（每空2分，共40分）

1．ISO 7498-2确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认。同时，ISO 7498-2也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换、业务填充机制、路由控制机制和公证机制。

2．古典密码包括 代替密码和置换密码两种，对称密码体制和非对称密码体制都属于现代密码体制。传统的密码系统主要存在两个缺点：一是 密钥管理与分配问题 ；二是 认证问题 。在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。

3．根据使用密码体制的不同可将数字签名分为 基于对称密码体制的数字签名 和 基于公钥密码体制的数字签名 ，根据其实现目的的不同，一般又可将其分为 直接数字签名 和 可仲裁数字签名 。

4. DES算法密钥是64位，其中密钥有效位是56位。RSA算法的安全是基于分解两个大素数的积的困难。

5．密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式有两种：一种是由中心集中生成，另一种是由个人分散生成。

6．认证技术包括站点认证、报文认证和身份认证，而身份认证的方法主要有口令、磁卡和智能卡、生理特征识别、零知识证明。

7．NAT的实现方式有三种，分别是静态转换、动态转换、端口多路复用。

8．数字签名是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

三、 简答题（每小题8分，共24分）

1、网络信息安全的含义？

答：网络信息安全是指利用[网络管理](http://baike.baidu.com/view/325702.htm" \t "_blank)控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可使用性受到保护。计算机网络安全包括两个方面，即[物理安全](http://baike.baidu.com/view/3153048.htm" \t "_blank)和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安安全包括信息的完整性、保密性和可用性。

2、什么是入侵检测系统？

答：[入侵检测](http://baike.baidu.com/view/16487.htm" \t "_blank)系统（简称“IDS”）是一种对[网络传输](http://baike.baidu.com/view/1542295.htm" \t "_blank)进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的[网络安全](http://baike.baidu.com/view/17495.htm" \t "_blank)设备。它与其他网络安全设备的不同之处便在于，IDS是一种积极主动的安全防护技术。 IDS最早出现在1980年4月。 1980年代中期，IDS逐渐发展成为入侵检测专家系统（IDES）。

3、请说明DES算法的基本过程？

答：DES加密算法特点：分组比较短、密钥太短、密码生命周期短、运算速度较慢。

DES工作的基本原理是，其入口参数有三个:key、data、mode。 key为加密解密使用的密钥，data为加密解密的数据，mode为其工作模式。当模式为加密模式时，明文按照64位进行分组，形成明文组，key用于对数据加密，当模式为解密模式时，key用于对数据解密。实际运用中，密钥只用到了64位中的56位，这样才具有高的安全性。

四、 分析题（16分）

1．下图表示的是P2DR2动态安全模型，请从信息安全安全角度分析此模型？

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

## 8．PKI支持的服务不包括＿＿＿。

## A. 非对称密钥技术及证书管理 B. 目录服务

## C. 对称密钥的产生和分发 D. 访问控制服务

9．设哈希函数H有128个可能的输出(即输出长度为128位)，如果H的k个随机输入中至少有两个产生相同输出的概率大于0.5，则k约等于＿＿。

A．2128 B．264

C．232 D．2256

10．Bell-LaPadula模型的出发点是维护系统的＿＿＿，而Biba模型与Bell-LaPadula模型完全对立，它修正了Bell-LaPadula模型所忽略的信息的＿＿＿问题。它们存在共同的缺点：直接绑定主体与客体，授权工作困难。

A．保密性 可用性 B．可用性 保密性

C．保密性 完整性 D．完整性 保密性

二、 填空题（每空2分，共40分）

1．ISO 7498-2确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认。同时，ISO 7498-2也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换、业务填充机制、路由控制机制和公证机制。

2．古典密码包括 代替密码和置换密码两种，对称密码体制和非对称密码体制都属于现代密码体制。传统的密码系统主要存在两个缺点：一是 密钥管理与分配问题 ；二是 认证问题 。在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。

3．根据使用密码体制的不同可将数字签名分为 基于对称密码体制的数字签名 和 基于公钥密码体制的数字签名 ，根据其实现目的的不同，一般又可将其分为 直接数字签名 和 可仲裁数字签名 。

4. DES算法密钥是64位，其中密钥有效位是56位。RSA算法的安全是基于分解两个大素数的积的困难。

5．密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式有两种：一种是由中心集中生成，另一种是由个人分散生成。

6．认证技术包括站点认证、报文认证和身份认证，而身份认证的方法主要有口令、磁卡和智能卡、生理特征识别、零知识证明。

7．NAT的实现方式有三种，分别是静态转换、动态转换、端口多路复用。

8．数字签名是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

三、 简答题（每小题8分，共24分）

1、网络信息安全的含义？

答：网络信息安全是指利用[网络管理](http://baike.baidu.com/view/325702.htm" \t "_blank)控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可使用性受到保护。计算机网络安全包括两个方面，即[物理安全](http://baike.baidu.com/view/3153048.htm" \t "_blank)和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安安全包括信息的完整性、保密性和可用性。

2、什么是入侵检测系统？

答：[入侵检测](http://baike.baidu.com/view/16487.htm" \t "_blank)系统（简称“IDS”）是一种对[网络传输](http://baike.baidu.com/view/1542295.htm" \t "_blank)进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的[网络安全](http://baike.baidu.com/view/17495.htm" \t "_blank)设备。它与其他网络安全设备的不同之处便在于，IDS是一种积极主动的安全防护技术。 IDS最早出现在1980年4月。 1980年代中期，IDS逐渐发展成为入侵检测专家系统（IDES）。

3、请说明DES算法的基本过程？

答：DES加密算法特点：分组比较短、密钥太短、密码生命周期短、运算速度较慢。

DES工作的基本原理是，其入口参数有三个:key、data、mode。 key为加密解密使用的密钥，data为加密解密的数据，mode为其工作模式。当模式为加密模式时，明文按照64位进行分组，形成明文组，key用于对数据加密，当模式为解密模式时，key用于对数据解密。实际运用中，密钥只用到了64位中的56位，这样才具有高的安全性。

四、 分析题（16分）

1．下图表示的是P2DR2动态安全模型，请从信息安全安全角度分析此模型？

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

## 8．PKI支持的服务不包括＿＿＿。

## A. 非对称密钥技术及证书管理 B. 目录服务

## C. 对称密钥的产生和分发 D. 访问控制服务

9．设哈希函数H有128个可能的输出(即输出长度为128位)，如果H的k个随机输入中至少有两个产生相同输出的概率大于0.5，则k约等于＿＿。

A．2128 B．264

C．232 D．2256

10．Bell-LaPadula模型的出发点是维护系统的＿＿＿，而Biba模型与Bell-LaPadula模型完全对立，它修正了Bell-LaPadula模型所忽略的信息的＿＿＿问题。它们存在共同的缺点：直接绑定主体与客体，授权工作困难。

A．保密性 可用性 B．可用性 保密性

C．保密性 完整性 D．完整性 保密性

二、 填空题（每空2分，共40分）

1．ISO 7498-2确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认。同时，ISO 7498-2也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换、业务填充机制、路由控制机制和公证机制。

2．古典密码包括 代替密码和置换密码两种，对称密码体制和非对称密码体制都属于现代密码体制。传统的密码系统主要存在两个缺点：一是 密钥管理与分配问题 ；二是 认证问题 。在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。

3．根据使用密码体制的不同可将数字签名分为 基于对称密码体制的数字签名 和 基于公钥密码体制的数字签名 ，根据其实现目的的不同，一般又可将其分为 直接数字签名 和 可仲裁数字签名 。

4. DES算法密钥是64位，其中密钥有效位是56位。RSA算法的安全是基于分解两个大素数的积的困难。

5．密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式有两种：一种是由中心集中生成，另一种是由个人分散生成。

6．认证技术包括站点认证、报文认证和身份认证，而身份认证的方法主要有口令、磁卡和智能卡、生理特征识别、零知识证明。

7．NAT的实现方式有三种，分别是静态转换、动态转换、端口多路复用。

8．数字签名是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

三、 简答题（每小题8分，共24分）

1、网络信息安全的含义？

答：网络信息安全是指利用[网络管理](http://baike.baidu.com/view/325702.htm" \t "_blank)控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可使用性受到保护。计算机网络安全包括两个方面，即[物理安全](http://baike.baidu.com/view/3153048.htm" \t "_blank)和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安安全包括信息的完整性、保密性和可用性。

2、什么是入侵检测系统？

答：[入侵检测](http://baike.baidu.com/view/16487.htm" \t "_blank)系统（简称“IDS”）是一种对[网络传输](http://baike.baidu.com/view/1542295.htm" \t "_blank)进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的[网络安全](http://baike.baidu.com/view/17495.htm" \t "_blank)设备。它与其他网络安全设备的不同之处便在于，IDS是一种积极主动的安全防护技术。 IDS最早出现在1980年4月。 1980年代中期，IDS逐渐发展成为入侵检测专家系统（IDES）。

3、请说明DES算法的基本过程？

答：DES加密算法特点：分组比较短、密钥太短、密码生命周期短、运算速度较慢。

DES工作的基本原理是，其入口参数有三个:key、data、mode。 key为加密解密使用的密钥，data为加密解密的数据，mode为其工作模式。当模式为加密模式时，明文按照64位进行分组，形成明文组，key用于对数据加密，当模式为解密模式时，key用于对数据解密。实际运用中，密钥只用到了64位中的56位，这样才具有高的安全性。

四、 分析题（16分）

1．下图表示的是P2DR2动态安全模型，请从信息安全安全角度分析此模型？